Technologies with the potential to enhance resilience - An overview on the activities of ENISA

Demosthenes.Ikonomou@enisa.europa.eu

5th International Conference on Critical Information Infrastructures Security

About Resilience

- Resilient are the networks that provide and maintain an acceptable level of service in face of faults affecting their normal operation.
- The main aim of the resilience is for faults to be invisible to users.

About Resilience

- Improving the resilience of a network is an issue of risk management which includes :
  - risk identification;
  - evaluation and;
  - acceptance or mitigation.
- A wide accepted list of risks to the resilience of networks includes :
  - flash crowd events
  - cyber attacks
  - outages of other support services
  - natural disasters and
  - system failings
- The mitigation of identified risks involves technical measures such as :
  - resilient design
  - resilient transmission media
  - resilient equipment and
  - technologies that improve resilience

Why ENISA?

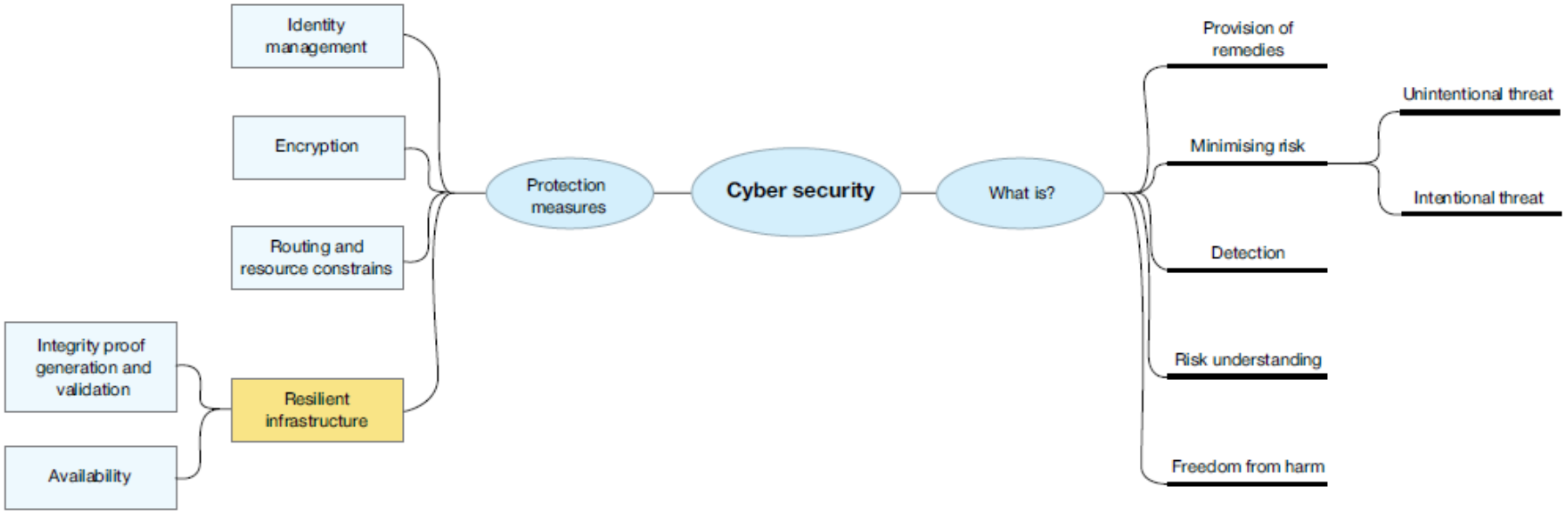
- EC Communication on CIIP - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience“, March 2009;
- ENISA is addressing the following areas:
  - Regulatory and policy aspects;
  - Network operators practices;
  - Technologies with a potential to improve resilience characteristics of networks;

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

Video on Importance of Resilience

http://www.youtube.com/user/enisasta

Simplification of ITU-T ontological model of cyber-security stressing resilience



Gap analysis in standardisation

- Definition of resilience
  - ETSI TR 102 445 – Emergency issues
  - ISO/IEC 27*, BS 25999 – Business Continuity Management
- Technical standards
- Some metrics
  - ITU-T: IP service availability, IP Packet Loss Ratio, IP Packet Transfer Delay, IP Packet Delay Variation, …
  - IETF: IP Packet Delay Variation, One-Way Packet Loss, …

Gap analysis in standardisation

- Promote work items in the SDOs to support the specification of metrics and supporting test and validation criteria to be used in the assessment of resilience;
- Promote work items in the SDOs to support the development of a taxonomy for resilience;
- Encourage telco SDOs to build links from their work to the output of bodies dealing with ancillary features (eg, power, environmental control, etc.);
- Add ‘resilience’ as a ‘keyword’ in classifying standards in the SDOs;
- Update SDOs procedures in approving work items to address how resilience will be achieved, e.g. in case a system fails;

Technologies with a potential to have an impact in terms of resilience

- cloud computing;
- real-time detection & diagnosis systems;
- future wireless networks, adhoc networks;
- smart grids and SCADA;
- sensor networks;
- supply chain integrity (SCI);
- interconnected networks;

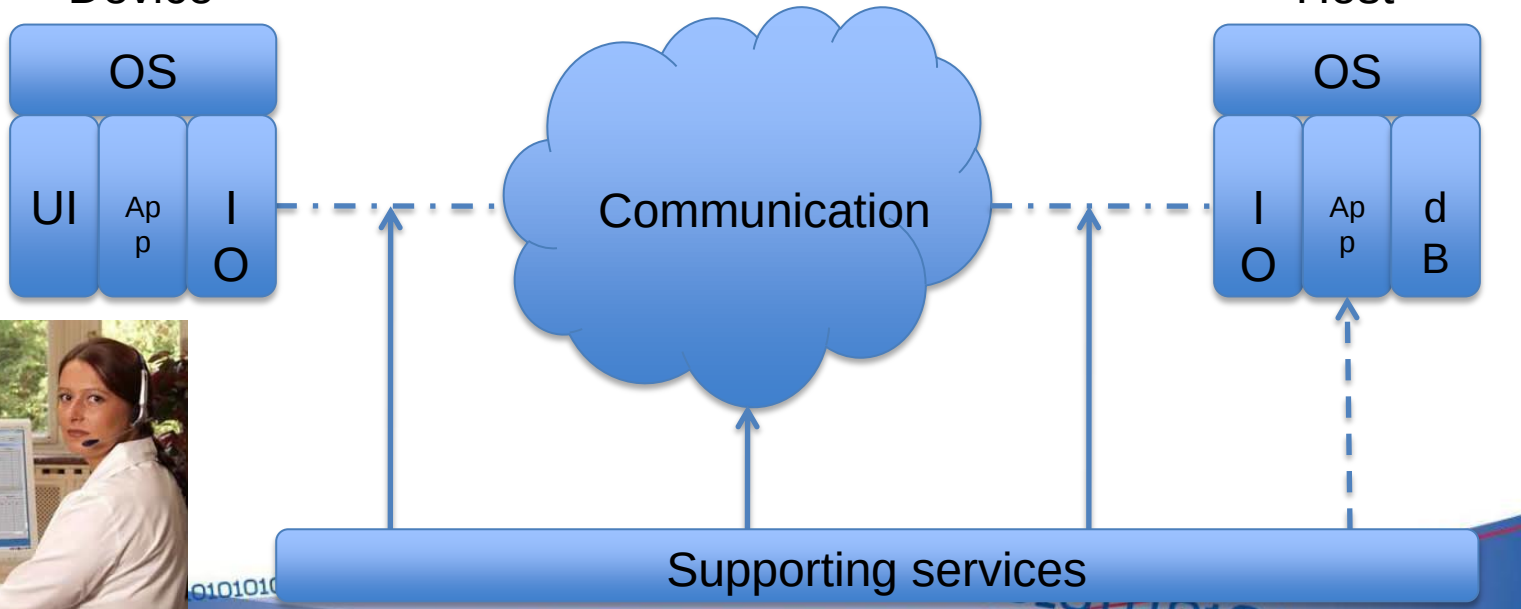
PROCENT

- Priorities of research on current and emerging network trends
- Assessment of the impact of new technologies
- Identification of need for research
- Areas of biggest interest
  - Cloud Computing
  - Real-Time Detection and Diagnosis Systems
  - Future Wireless Networks
  - Sensor Networks
  - Integrity of Supply Chain

End-to-end (e2e) resilience

Device

Host



DNSSEC activities of ENISA

- 2008
  - Survey Deployment Status;
  - Paper on the security features and the problems it solves;
  - Stocktaking operators on the perceived security enchantments.
- 2009
  - Study costs of deployment;
  - Good Practice Guide on deploying DNSSEC.
- 2010
  - Pilot actions;
  - Create end user // educational // promotional material.

ENISA Special Session

- *'Cyberwar ante portas! Identifying the role of the academic community in national cyber defence exercises'*, Prof. D. Gritzalis from AUEB, Athens;
- *'Quality of Resilience Metrics: State-of-the-Art and Future Trends'*, Dr. Chold, AGH University of Science and Technology, Kraków, Poland;
- Panel Discussion;

Further information

European Network and Information Security Agency

Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu
https://www.enisa.europa.eu/act/res/technologies